State of Idaho

Information Technology Services
Office of the Governor

BRAD LITTLE
Governor
JEFF WEAK
Administrator
GREG ZICKAU
Deputy Administrator/
Chief Information Officer

11331 W. Chinden Blvd., #B201
Boise, ID 83714
P.O. Box 83720
Boise, ID 83720-0042
Telephone (208) 605-4064 or FAX (208) 605-4090
http://its.idaho.gov

TO: Alex Adams, Director DFM
Chair, Coronavirus Financial Advisory Committee

FROM: Jeff Weak, Administrator

DATE: October 21, 2020

SUBJECT: IT Proposal for CFAC

REQUEST: CARES Act funds to strategically position the state – request $4,728,933

Background:
COVID-19 profoundly changed how Idaho State Government operates. The demands generated by a work-from-home workforce have placed unprecedented stress on the state's IT infrastructure. Virtual Private Network (VPN) users increased 532%. Bandwidth utilization is up 320%. Although ITS rose to the challenge to meet these increased demands, the current infrastructure failed to keep up and the state endured several outages as a result. The state's IT infrastructure must be robust and resilient enough to handle the current remote workload and scale for future circumstances that could warrant a similar response.

Purpose and Goals:
This strategy was carefully crafted to provide immediate relief for current issues and build sufficient capacity to meet anticipated future needs. A primary focus is to simplify the network architecture, making it easier to manage while improving cybersecurity by reducing our attack surface. We were fortunate to receive CARES funding to replace some bandwidth limiting network devices, a complete overhaul of the state's firewall, and new tools that enable technicians to support this critical technology from remote locations.

This request is complementary to our previous initiatives and lays the critical groundwork to rapidly expand the state's hybrid datacenter by addressing key power constraints and by leveraging both on premise hardware and commercial cloud solutions. The highly virtualized environment also provides agility with on-demand compute power, enabling us to shift resources when and where needed. An example of this was the Rebound.Idaho website. To meet the demands to accommodate an

anticipated 140,000 concurrent users, ITS was able to increase compute power in *minutes* alleviating potential problems. As a result, the site performed flawlessly with no latency or downtime.

Maybe most importantly, this strategy dramatically improves cybersecurity for the state. The appliances and tools identified correct deficiencies and add critical capability to our security stack. These measures ensure our citizens personal data is safeguarded to highest degree possible.

This plan also includes substantial amount of professional services. This additional support is crucial to ensure best possible outcomes and that implementation is executable within the tight timeframes associated with the funding.

Executive summary for items requested:
The individual initiatives have been consolidated into four main themes that will enable ITS to meet technology demands for the state.

Network and Infrastructure *$2,309,033*
ITS currently supports a complex statewide network with significant demands on its infrastructure. This infrastructure is a mix of equipment from several different vendors, much of which was designed to meet the needs of an individual agency (pre-IT Modernization). Considerable amounts of this hardware is out of date and unsupported by vendors, which creates increased risk for outages and significant threats to security. The disparity in platforms, hardware lifecycles, licensing models, and expertise of ITS staff on the various platforms, all come together to create a perfect storm of challenges in delivering a stable, consistent network services. This funding will allow ITS to implement standardized solutions both from a hardware and software licensing perspective.

This solution also accounts for enhanced administrative applications and asset management tools. COVID resulted in most of our state employees moving to remote work, taking their state-provided computers home with them. Accurate tracking of these assets is critical for agencies to control costs and ensure accurate management of the investment the state has made in IT hardware. In addition to precise accountability, technicians will be able to handle most user requests remotely, negating the need to physically touch a device.

Two critical lessons learned in responding to the pandemic is that we must be much faster at bringing new computers into service and that we must minimize physical contact with the computer and customer as much as possible. ITS provisions and deploys devices for nearly 7000 customers across its supported agencies. When new devices are brought into service, technicians must manually configure the operating system and load specific agency applications. This “hi-touch” approach slowed the placement of new devices to the customer just as the pandemic demanded we expand the remote workforce with new devices. This overwhelmed ITS technical capacity and unnecessarily stressed both ITS personnel and customers at a critical time. The tools

requested allow ITS technicians to handle endpoint provisioning in a zero-touch fashion, meaning the device goes straight to the customer from the factory and configuration changes are applied when the customer connects with their new device.

Following COVID best practices, this solution no longer requires technicians to visit users in person and will significantly reduce staff exposure between agencies. Additionally, this solution dramatically cuts provisioning times an estimated four hours per device and will allow ITS to apply an additional 7,000 hours per year to closing higher priority jobs for our customers.

Security and compliance *$2,300,600*

With the huge shift to a remote workforce, there has been a significant increase in malicious attempts to compromise government sector networks worldwide. As a result, there is a growing need to deploy enhanced threat detection tools throughout the state. These capabilities are critical in detecting threats and implementing proactive measures.

A major focus is the replacement our email gateway. The current solution has been overwhelmed with the shift to remote work, significantly increasing employee's reliance upon email. Our current gateway processes over 6 million incoming messages a month, often exceeding its capacity. Additionally, of the messages processed each month, nearly 1 million were filtered out for malicious content. Email is the most popular vector for nearly all cyber threats. Replacing the email gateway is a huge boost to the cybersecurity posture of the state.

This solution also enables us to maximize the features of our new firewalls by enabling advanced alerting, threat detection, and automated threat response capabilities available with the platform.

Professional Services *$119,300*

Professional services are critical to ensuring ITS can execute all CARES Act funding with the existing timeline. It will bring in additional resources with advanced technical skills specific to the technologies previously identified. These experts will ensure optimum configuration of equipment, reduce implementation times and provide ITS staff firsthand experience in learning the new tools.

Proposed Implementation:

Engineering/Procurement Phase: Oct 2020
Solidify professional services contracts with vendor partners. Design final engineering solution. Work closely with DOP to submit all purchase orders with expedited delivery (as necessary).

Implementation Phase: Nov – Dec 2020
Execute project management plan with professional services teams for all scheduled projects. Integrate with ITS Chief of Operations, Chief Technology Officer, Enterprise

Architect and Project Managers to maximize team effectiveness, meet timelines and ensure success.

Although efforts will run simultaneous at times, the priorities will be:

1. Firewalls and other cybersecurity systems (already approved)
2. Network upgrades
3. Security Operations tools